

REMARKS

Claims 1-20 are pending. All stand rejected. The applicant has amended claims 1, 8, 10 and 20. The applicant requests further examination and consideration in view of the amendments above and remarks set forth below.

Specification:

The disclosure was objected to due to a minor informality in the third paragraph of the summary of the invention. The applicant has amended the specification to correct the informality.

In addition, the applicant has amended the specification to correct a minor typographical error at page 10, line 34. More particularly, "Hyer" is replaced with "Hyper." No new matter has been entered.

Claim Objection:

Claim 8 was objected to due to a minor informality in which the phrase "is conflict" should be "is in conflict." The applicant has amended claim 8 to correct the informality.

Rejection under 35 U.S.C. § 112:

Claim 10 was rejected as being indefinite. More particularly, the examiner stated that it is unclear whether the applicant wishes to claim that at least one network type is an abstract type or exactly one network type is abstract.

The applicant has amended claim 10 to recite that at least one of the network types is an abstract type. The applicant notes that no prior art has been applied against claim 10. Moreover, as explained below, claim 10 depends from an allowable base claim 1. Therefore, claim 10 is allowable.

Rejections under 35 U.S.C. § 102:

Claims 1-4, 13, 15, 17, 18 and 20 were rejected as being unpatentable over U.S. Patent No. 5,968,176 issued to Nessett et al. (hereinafter "Nessett").

The present invention as recited in claims 1-4, 13, 15, 17, 18 and 20 is directed toward a method and apparatus for configuring a network security system. As is explained in the applicant's summary of the invention:

...A registry data structure includes useful information about the network, such as definitions of roles within the network. The registry may also include information regarding the topology of the network. Documents that contain network security policies are linked to the registry data structure. The policy documents may then be transformed into device-specific configuration documents using a document transformation algorithm, which takes a document of a certain format as input and generates a document in a different format as output. Various different scripts may control the transformation process to achieve compatibility with security devices from different vendors. An advantage of the invention is that major network management tasks, including policy enforcement, may be done by document transformations. Once adopted, a security strategy may be changed in order to adapt to changing business requirements.

Applicant's specification at page 3, lines 11-23. Accordingly, applicant's claim 1 recites a method of configuring a network security system, comprising: forming a registry data structure for defining roles within a network; mapping network security policies to the registry data structure, said network security policies being contained in one or more policy documents stored in machine readable form; and using a document transformation algorithm to transform the policy documents into one or more device-specific configuration documents stored in machine-readable form. As is further explained in the applicant's summary of the invention:

...Preferably, information including network security policies, role definitions and topology information are in the form of documents, such as Extensible Markup Language (XML) documents. XML Stylesheet Transformation (XSLT) is preferably used to transform the XML documents into formats appropriate for configuring the actual devices used in the network to implement the desired security policies. While another document format language can be used, an advantage of using an industry standard document format language, such as XML, is that the invention can be implemented using open-standard tools. For example, XML and XSLT parsers and processors are widely available.

Applicant's specification at page 3, lines 24-33. Thus, the applicant has amended claim 1 to clarify that the one or more policy documents are in a standard document format language. XML is a specific example of a standard document format language.

Nesbett does not suggest or disclose the use of a standard document format language for security policy documents and the transformation of those documents into device-specific configuration documents, as is required by the applicant's amended claim 1. Rather, Nesbett discloses that "security policy statements" are

interpreted by a script interpreter. Nessett, at col. 4, lines 10-20 and 47-55. Thus, Nessett suffers from similar drawbacks of other prior art approaches discussed in the applicant's background of the invention in that the approach of Nessett lacks scalability is unable to make use of open-standards document management tools.

For at least this reason, amended claim 1 is allowable over Nessett. Claims 2-4, 13, 15, 17, 18 are allowable at least because they depend from claim 1.

Independent claim 20 recites that each security policy document is in a standard document format language. Claim 20 is allowable at least because Nessett does not suggest or disclose the use of a standard document format language for security policy documents.

Rejections under 35 U.S.C. § 103:

Claims 5-9, 11 and 12 were rejected as being unpatentable over Nessett in view of The Open Group, "Authentication and Security Services – Introduction to Security Services", pages 44-56, 1997 (hereinafter, "The Open Group").

As explained above, claim 1 is allowable over Nessett at least because Nessett does not suggest or disclose the use of a standard document format language for security policy documents. The Open Group does not suggest or disclose this feature either. Thus, claims 5-9, 11 and 12 are allowable over Nessett and The Open Group, taken singly or in combination.

Claims 14 and 16 were rejected as being unpatentable over Nessett in view of Cheung, et al., "Distributed and Scalable XML Document Processing Architecture for E-Commerce Systems" (hereinafter "Cheung").

As explained above in reference to claim 1, Nessett does not suggest or disclose all of the features of claim 1. Cheung does not suggest or disclose the features of claim 1 that are missing from Nessett. Therefore, claim 1 is allowable over Nessett and Cheung, taken singly or in combination. Claims 14 and 16 are allowable at least because they are dependent from an allowable base claim 1.

Regarding Cheung, the examiner stated that Cheung discloses that XML is a good format to use and that it would have been obvious to one of ordinary skill in the art to combine the ideas of Cheung with the ideas of Nessett and use XML format for policy documents.

The applicant respectfully disagrees. While Cheung discloses the use of XML for data exchange in e-commerce systems, Cheung does not suggest or disclose the

use of a standard document format language for security policy documents, as is required by the applicant's claim 1, from which claims 14 and 16 depend. Cheung also does not suggest or disclose the transformation of such security policy documents into device-specific configuration documents, as is also required by the applicant's amended claim 1. Further, Cheung also does not suggest or disclose the use of XML for security policy documents, as is required by applicant's claim 14, nor does Cheung suggest or disclose the use of XLST for transformation of security policy documents, as is required by applicant's claim 16.

Specifically, Cheung teaches a document processing architecture for e-commerce systems. Title of Cheung. As is explained in Section 3.1 of Cheung, a Document Integrator (DI) is responsible for receiving input XML data from an application program. The DI processes the input file accord to script files written by the application programmer. According to the logic described in the script file, the DI communicates with various Transformation Modules (TM), passing to them appropriate XML documents. The documents returned from the TM's are also XML documents. The DI may temporarily store the returned documents for further processing or may pass these temporary XML files to other TM's as necessary. After collecting all the results from the TM's, the DI combines them and returns the final result to the application program.

Because Cheung only discusses the use of XML in connection with e-commerce systems, Cheung cannot suggest the use of XML for security policy documents. The examiner has not pointed out where in Nessett and Cheung a motivation or suggestion can be found to combine the references in a way that achieves the applicant's claimed invention.

Further, Cheung teaches in Section 5.1 that "there is essentially no restriction of location and platform of the servers where DI and TM's run" except that "the servers must support TCP/IP and should not be blocked by any firewall." Thus, to the extent that Cheung discusses network security at all, it is to point out that the architecture of Cheung is incompatible with network security devices. Therefore, a person would not have been motivated to utilize the teachings of Cheung for configuring a network security system.

This is another reason why claim 1 is allowable over Nessett and Cheung, taken singly or in combination and, thus, also another reason why Claims 14 and 16 are allowable.

Claim 19 was rejected as being unpatentable over Nessett in view of Cheung and in further view of Kay, Michael H., XSLT Programmer's Reference, Chapter "XSLT Part 2 – How Does XSLT Transform XML?", Wrox Books, February 20, 2001 (hereinafter "Kay"). As explained above, the applicant's claim 1 is allowable over Nessett and Cheung at least because neither Nessett, nor Cheung discloses the use of a standard document format language for security policy documents and the transformation of those documents into device-specific configuration documents. Kay does not suggest or disclose these features either. Accordingly, claim 1 is allowable over the references taken singly or in combination. Claim 19 is allowable at least because it is dependent from an allowable base claim 1.

Conclusion:

In view of the above, the applicants submit that all of the pending claims are now allowable. Allowance at an early date would be greatly appreciated. Should any outstanding issues remain, the examiner is encouraged to contact the undersigned at (408) 293-9000 so that any such issues can be expeditiously resolved.

Respectfully Submitted,

Dated: Jan. 7, 2005



Derek J. Westberg (Reg. No. 40,872)